Hindawi
Security and Communication Networks
Volume 2021, Article ID 6571700, 10 pages
https://doi.org/10.1155/2021/6571700

Research Article

pKAS: A Secure Password-Based Key Agreement Scheme for the Edge Cloud

Ping Liu,[1] **Syed Hamad Shirazi**,[2] **Wei Liu**,[1] **and Yong Xie**[1]

[1]*Department of Computer Technology and Application, Qinghai University, Xining, China*
[2]*Department of Information Technology, Hazara University, Baffa, Pakistan*

Correspondence should be addressed to Yong Xie; mark.y.xie@qq.com

Received 5 September 2021; Accepted 5 October 2021; Published 18 October 2021

Academic Editor: Xiaolong Xu

For the simplicity and feasibility, password-based authentication and key agreement scheme has gradually become a popular way to protect network security. In order to achieve mutual authentication between users and edge cloud servers during data collection, password-based key agreement scheme has attracted much attention from researchers and users. However, security and simplicity are a contradiction, which is one of the biggest difficulties in designing a password-based key agreement scheme. Aimed to provide secure and efficient key agreement schemes for data collecting in edge cloud, we propose an efficient and secure key agreement in this paper. Our proposed scheme is proved by rigorous security proof, and the proposed scheme can be protected from various attacks. By comparing with other similar password-based key agreement schemes, our proposed scheme has lower computational and communication costs and has higher security.

1. Introduction

With the dawn of the Internet of everything, Internet of things (IoT) has become to obtain the leading strategic position in research and development in the world. Even though various countries in the world pay attention to the development of the IoT, the influx of diverse traffic and the need of diversified application scenario has not only put forward new challenge for the centralized cloud computing architecture nowadays but also drove the emergence of the cloud computing paradigm [1, 2].

In the era of Internet of Things, mobile devices are no longer simple mobile phones, tablets, etc., but include more abundant augmented/virtual reality devices, intelligent medical device, and moving vehicle. The application scenario also transfers from voice/video communication and other services to virtual space experience, intelligent manufacturing, and the Internet of vehicles [3, 4]. In cloud-based services, data transmission speed will be affected by network traffic, and heavy traffic will lead to long transmission time, thus increasing power consumption cost. Therefore, the adoption of mobile edge computing (MEC) can meet the needs of IoT devices.

As shown in Figure 1, the collection and processing of data is a very important part of the Internet of Things. However, all collected data will be transmitted to the cloud server and then rely on the server's computing power for data processing and analysis. This will cause the server to be heavily loaded and prone to failure or downtime. At the same time, the increase in the amount of data will also increase the cost of the storage server. In addition, because the network is limited by the network bandwidth and speed, the network bandwidth is put under pressure when a large amount of monitoring data is transmitted, and the data may have large transmission delays and packet loss during transmission. Edge computing data provides format conversion, caching, processing, analysis, and transmission services, and the load of cloud servers improves the efficiency of data processing. The edge cloud includes IoT gateways and collectors. These devices together form an edge node network and provide lightweight computing power for the edge layer of the system.

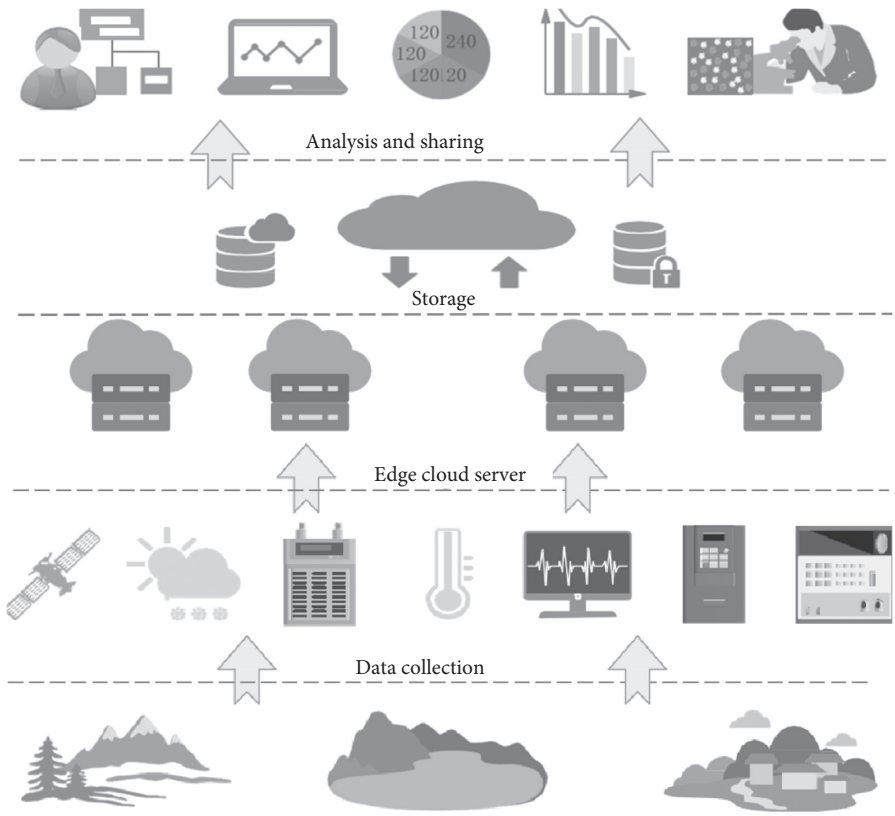

Figure 1: A typical data sharing model in edge cloud computing environment.

In the MEC-based Internet of Things, massive amounts of data are generated by a large number of sensors and various heterogeneous devices, and all storage devices are provided by different third-party vendors. Due to the distributed nature of MEC, data are stored in different network edges, which will increase the risk of data being attacked. For example, unauthorized users or opponents may modify or abuse the data uploaded in the storage, which will lead to data leakage and other problems. In order to solve these problems, this paper proposes identity verification based on password-based key agreement. This scheme can ensure both sides' identity authentication and data security.

In order to protect the data in the edge cloud from being tampered with, the administrator of the edge cloud server needs to authenticate with it when operating the server, so the sever can determine whether the administrator has been faked. To improve the security and verifiability of messages, Zheng [5] proposed a signcryption scheme, which can simultaneously sign and encrypt.

The key agreement protocol is the most commonly used method for two or more parties to communicate. Features of the protocol ensure that the data to be communicated are confidential, secure, and complete [6–10]. The protocol is to establish a session key jointly by two or more entities. The result of key agreement will be affected by any participant, and no trusted third party is required in the process. The session key is obtained by calculating the parameters generated by the participants. In order to enable both parties to authenticate each other, an authentication key agreement is proposed, and the protocol established a session key [11–13].

In 2005, the Diffie–Hellman key exchange in the encryption assumption protocol system is a secure and scalable authentication key exchange agreement, which performs key control and management during transmission [14–16]. In 2009, the elliptic curve cryptosystem (ECC) authentication scheme based on no pairing and few certificates was presented. The scheme was based on mobile devices communication and ID authentication with key agreement protocol. Furthermore, the proposed scheme is also to overcome more attacks [13, 17–20]. Many scholars believed that large prime numbers is difficult for hardware implementation of the elliptic curve cryptosystem, while the binary field was known as suitable [21, 22] in 2010–2012. In order to ensure the confidentiality and integrity of the sent and received messages, the authentication key agreement protocol must include a strong encryption algorithm. The key agreement protocol based on elliptic curve cryptography provides an important development for confidentiality, integrity, and user anonymity.

There are two types of key agreement protocols according to different authentication methods: password-based key agreement protocols and public-key-based key agreement protocols. The password-based authentication key agreement protocol was first proposed by Bellovin and Merritt [23]. In this protocol, both parties share a password in advance, which is used to authenticate each other's identity during communication and negotiate a short-term

session key. Public key-based key agreement can negotiate a session key through signature or public key verification. In this paper, password-based key agreement protocol is studied [15].

1.1. Motivations and Contributions. The proposed pKAS can ensure the security of the message and the authentication of the user identity when two parties communicate. We list our contributions as follows:

First, we put forward a secure password-based key agreement pKAS based on ECC for mutual authentication between the user and edge server. The proposed pKAS only needs to deliver the message twice, which greatly saves communication bandwidth. And, in this scheme, we use signcryption, signature verification, and hash operation etc., to ensure the confidentiality and integrity of the message, as well as the anonymity of the identity.

Second, we conduct strict security analysis on the proposed pKAS and compare it with other related schemes. The results show that the presented pKAS can resist various attacks.

Third, by comparing communication and calculation costs, the proposed pKAS has lower cost and is more secure than recent similar schemes.

1.2. Organization of the Paper. The structure of the paper is as follows. Sections 2 and 3 present the related works and the preliminaries. The system model and security requirements of the scheme proposed in this paper are shown in Section 4. Section 5 presents the proposed password-based key agreement scheme. Section 6 presents the performance and security analysis. Section 7 describes conclusion, future work, conflicts of interest, and data availability respectively.

2. Related Works

With the development of Internet technology, security in communications has become more and more significant. Therefore, how to identify remote users has become one of the most significant issues in the public network. In order to figure out the problem, many schemes have been presented. Lamport [24] first proposed the password-based scheme to ensure remote parties authentication scheme. Subsequently, many password-based key agreement schemes were proposed in [25–29].

In 2009, Xu et al. [25] presented an improved remote user authentication and key agreement scheme based on passwords and smart cards, and they certificated that their scheme is secure. Sood et al. [26] found that Xu et al.'s scheme is ineffective against password guessing attacks and impersonation attacks. Subsequently, Sood et al. put forward an improved authentication scheme. However, in 2012, Chen et al. [27] analyzed and pointed out that the scheme of Sood et al. only provided a single-party authentication function, and the legitimacy of the remote server was not authenticated. As a consequence, an improved key agreement scheme with stronger security was presented by Chen et al.\enleadertwodots, and the scheme achieved remote parties' authentication. Furthermore, they stated that their scheme could resist kinds of attacks. In those authentication schemes proposed by Sood et al., Chen et al., and many scholars [30–32], users must interact with the remote server to transmit information and repeat the login process and authentication process instead of completing the password change process on the client when he/she wants to change the password. In addition, these solutions will not find the wrong password entered during the login process. The wrong password can only be found in the final authentication process after a series of calculations and communications. Obviously, these schemes were inefficient and user-unfriendly, and failed to verify wrong password. Recently, Li et al. [28] analyzed that Chen et al.'s scheme could not ensure forward security and does not achieve perfect user anonymity. In addition, they proposed a scheme based on password and smart card, and the scheme can enhance remote user authentication and key agreement.

The message transmitted between the sender and the receiver may be eavesdropped by the adversary through public channels. The identity of users should be kept confidential during message transmission. Otherwise, the adversary will track the user by collecting the user's identity information. Some interesting bilinear pairing-based and ECC-based key agreement protocols were proposed in recent years [33–36]. Irshad et al. [33] presented the scheme which used bilinear pairing operations in the interaction between mobile devices and servers. A method that can use mobile devices to access the server was proposed by Tsai and Lo [35], but later proved that the scheme cannot resist impersonation attacks and man-in-the-middle attacks. It is a pity that Xiong et al. [37] believe that Irshad et al.'s scheme is very computationally expensive for mobile devices. The protocol based on ECC is more efficacious because point addition or multiplication in elliptic curves is more efficient than modular exponents. In addition, the elliptic curve encryption protocol which is based on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP) is more secure. In 2017, a lightweight password-base key agreement protocol was proposed by Mahmood et al. [34]. But later, the program was verified to have some security issues, such as no anonymity, no resistance to replay attacks, and no guarantee of data confidentiality. Recently, a key agreement scheme based on ECC was presented by Kaur et al. [36], and they stated their scheme can overcome many kinds of attacks. Nonetheless, we strictly analyzed and found the scheme of Kaur et al. proposed suffered from no resistance forgery attack and insider attack.

3. Preliminaries

3.1. One-Way Hash Function. Let message m be a message that requires a hash value. The length of m is a variable, while h is the fixed length. Given m, it is easy to obtain h. However, given h, it is infeasible to obtain m.

3.2. Elliptic Curve Cryptosystem (ECC). In 1985, the elliptic curve was used for data encryption by Miller firstly. Later, Koblitz based on the elliptic curve discrete logarithm problem (ECDLP) built a new encryption system, which is called the elliptic curve cryptosystem (ECC). ECC has lower computational overhead than other public key cryptographies such as RSA. Since then, ECC has been widely used in cryptographic protocols and security schemes. The following describes the basic knowledge of ECC and computational difficulties in ECC.

Elliptic curve cryptography is a public key cryptography method based on elliptic curve mathematics. The commonly used expression of elliptic curve in finite field F_p is: $y^2 = x^3 + ax + b(\mathrm{mod}p)$ $(a, b \in F_p,$ and $(4a^3 + 27b^2)(\mathrm{mod}p) \neq 0)$, all coefficients are elements in a finite field F_p (where p is a large prime number). Let $E_p(a, b)$ denotes the point set $\{(x, y)|0 \leq x < p,\ 0 \leq y < p,$ and x, y are both integers$\}$ on the elliptic curve defined by the equation and the infinity point O.

The addition on $E_p(a, b)$ is defined as follows:

For any point in $E_p(a, b)$, $P = P + O$.

Let Q, R be the two points in $E_p(a, b)$. $Q + R$ is defined as follows: draw a straight line passing through Q, R and the elliptic curve to intersect point P, then $Q + R = -P$.

Let Q be a point in $E_p(a, b)$, and the multiples of Q are defined as follows: draw a tangent to the elliptic curve at point Q, and set the tangent to intersect the elliptic curve at point S; then, $2 \cdot Q = Q + Q = -S$. Similarly, $n \cdot Q = Q + Q + \cdots + Q$ (n times), where $n \in Z_p$, $n > 0$.

3.3. Complexity Assumptions. The security foundation of ECC is an elliptic curve discrete logarithm problem (ECDLP), which can be defined as follows.

ECDLP: assume two random points P_1 and P_2 in (E/E_p), $P_2 = kP_1$, where $k \in Z_p^*$. It is easy to compute P_2 if knows k and P_1, while it is infeasible to compute k if knows P_1 and P_2.

4. System Model and Security Model

4.1. System Model. On analysis of the requirements of communication between the user and edge server, there are two types of roles related in our system, such as users communicating with server, a trust authority (TA) can be regarded as a completely trusted administrator and cannot be compromised by any adversary. With a view to user authentication and key agreement, a user (Assumed be U_i) must be registered in the TA, and then he/she can perform mutual authentication and key agreement with edge cloud server other users (such as U_j) only using the password and smart card.

The network model of our system can be illustrated in Figure 2. Before the users communicate with the edge server, the users must register with the TA through a secure channel and store the corresponding registration information on her/his smart cards. After successful registration, users can perform mutual authentication and key negotiation through edge server and implement operations such as secure data management on the edge cloud.

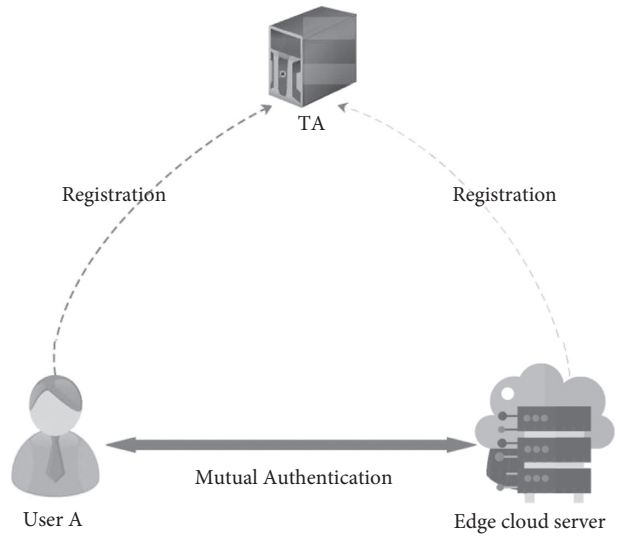

Figure 2: A typical key agreement model in edge cloud computing environment.

4.2. Security Requirements. Before analyzing security requirements, let us assume adversary's capabilities based on the application. An adversary $\mathscr{A}$ generally contains the following capabilities:

(i) The open channel can be controlled by $\mathscr{A}$, that is to say, the messages through the open channel $\mathscr{A}$ can be deleted, intercepted, modified, and resent

(ii) $\mathscr{A}$ can traverse the password space in polynomial time, that is, if it has known any other secret information, $\mathscr{A}$ can guess the password by brute force attack

(iii) $\mathscr{A}$ can obtain the user's password through a malicious terminal and can also extract data that are stored in smart card

On the capacities of the adversary $\mathscr{A}$, the security requirements of password-based key agreement scheme should include forward secrecy and must be resistant to know attacks, such as offline password guessing attack, replay attack, user impersonation attack, server spoofing attack, and parallel attack. Furthermore, the scheme must be mutual authentication and anonymity.

5. The Proposed Scheme (pKAS)

In this section, a key agreement scheme based on password (called pKAS for short) by using ECC was proposed. There are no bilinear paring operations in pKAS. Overall, pKAS has four phases: system initial phase, registration phase, login and key agreement phase, and offline password change phase. For simplicity, we list the symbols used in this paper and their corresponding meanings in Table 1.

Next, the following sections present the four phases of the proposed scheme.

5.1. System Initialization Phase. Trust authority (TA) is responsible for the system initialization phase. In this phase,

Table 1: Description of the symbols used.

Symbol	Description
TA	The trust authority
ID_i	The identity of user U_i
p	A big prime
$E_p(a,b)$	Point set of an elliptic curve: $y^2 = x^3 + ax + b \bmod p$
κ	A middle large integer
Δt	The limited time interval
P	The base point of the elliptic curve
G	A finite cycle additive group over the elliptic curve
$h(\cdot)$	One-way hash function
x_i	The secret key of user U_i
X_i	$X_i = x_i P$, the public key of user U_i

TA selects a big prime p; then, in finite field, F_p constructs a nonsingular ecliptic curve $E_p(a,b)$ and chooses base points P on $E_p(a,b)$ and generates a finite cycle additive group G of order q with P.

5.2. Registration Phase. Users, edge cloud sever, and TA complete the registration phase together. Assume the current user U_i's identity be ID_i, the registration is completed as follows:

Step R1: U_i sets his password PW_i, then chooses a random number $x_i, a_{i0} \in Z_q^*$, and computes $X_i = x_i P$, $a_{i1} = h(PW_i \| a_{i0})$, $a_i = h(h(ID_i) \oplus a_{i1} \bmod \kappa)$. At last, U_i sends $\{ID_i, X_i\}$ to TA in a channel that an adversary cannot eavesdrop on.

Step R2: when TA receives $\{ID_i, X_i\}$, it will store $\{ID_i, X_i\}$ in the server.

5.3. Login and Key Agreement Phase. We assume there are two users, user U_i and edge cloud sever U_j in this phase. They login by using their ID and password, then authenticate, and consult with session key each other.

Step A1: U_i inputs his/her ID_i' and PW_i', then smart cart computes $a_i' = h(h(ID_i) \oplus h(PW_i' \| a_{i0}) \bmod \kappa)$, and checks whether $a_i' = a_i$ holds or not. If it does not, the session is terminated.

Step A2: U_i randomly chooses $c_i \in Z_q^*$, computes $C_i = c_i P$, $PID_i = ID_i \oplus h(c_i X_j \| t_i)$, $f_i = h(ID_i \| ID_j \| PID_i \| C_i \| t_i)$, where t_i is current timestamp, $\sigma_i = c_i + x_i f_i \bmod q$. At last, U_i sends $M_1 = \{C_i, PID_i, t_i, \sigma_i\}$ to U_j.

Step A3: after receiving $\{C_i, PID_i, PID_j, t_i, \delta_i\}$, U_j checks whether $t_j - t_i < \Delta t$, if not, U_j terminates the session, else U_j computes $ID_i^* = PID_i \oplus h(x_j C_i \| t_i)$, $f_i{}' = h(ID_i^* \| ID_j \| PID_i \| C_i \| t_i)$ and checks whether $C_i = \sigma_i P - f_i' X_i$ holds or not. If not, U_j terminates the session. U_j chooses $C_j \in Z_q^*$ and computes $C_j = c_j P$, $sk_{ji} = h(ID_i \| ID_j \| t_i \| t_j \| C_i c_j)$, $f_j = h(ID_i \| C_i c_j \| sk_{ij} \| t_i \| t_j \| ID_j)$, $\delta_j = C_j + x_j f_j \bmod q$. At last, U_j sends $M_2 = \{C_j, f_j, \delta_j, t_j\}$ to U_i.

Step A4: after receiving $\{C_j, f_j, \sigma_j, t_j\}$ from U_j, U_i checks whether current timestamp t_i' meets $t_i' - t_j < \Delta t$ or not, if not, U_i terminates the session, else U_i computes $C_j' = \sigma_j P - f_j X_j$, $sk_{ij} = h(ID_i \| ID_j \| t_i \| t_j \| c_i C_j)$ and checks whether $f_j = h(ID_i \| C_i \| C_j \| sk_{ji} \| t_i \| t_j \| ID_j)$ holds or not. If not, U_i terminates the session, else U_i accepts this session.

At last, U_i and U_j have agreed an identical session key $sk_{ji} = sk_{ij}$. Figure 3 presents the flowchart of login and key agreement phase.

5.4. Offline Password Change Phase. In order to obtain a better user experience, while meeting the high requirements of security and efficiency, the user can complete this phase locally in the proposed scheme as follows:

Step C1: in order to verify the user's identity, the user must enter ID_i, PW_i in the smart card.

Step C2: the smart card computes $a_i' = h(hID_i) \oplus h(PW_i' \| a_{i0}) \bmod \kappa$ and checks if a_i' and a_i are equal. If not, the system will terminate the session. Else, it means the correctness of ID_i and PW_i is $\kappa - 1/\kappa \approx 99.61/100$, $\kappa = 2^8$, and it can go to the next step.

Step C3: user U_i inputs new password PW_i^{new} and computes $a_i = h(h(ID_i) \oplus h(PW_i^* \| a_{i0}) \bmod \kappa)$.

6. Security and Performance Analysis

Security analysis and proof of our scheme is presented in this section. As well as the proposed pKAS is proven to be able to resist all kinds of attacks. Besides, we analyze and compare the communication calculation and bandwidth consumption of similar schemes.

6.1. Security Analysis. In this section, the details of security analysis are described as following.

Proposition 1. *The proposed pKAS scheme can be secure against offline password guessing attack.*

Proof. Assume an adversary $\mathcal{A}$ has got U_i's smart card and obtained the data stored in the card. he/she can launch password guessing attack by the following steps:

Step D1: $\mathcal{A}$ guesses PW_i^* from password dictionary space and ID_i from identity diction space

Step D2: $\mathcal{A}$ retrieves a_{i0} and a_i and computes $a_i' = h(h(ID_i) \oplus h(PW_i^* \| a_{i0}) \bmod \kappa)$

Step D3: $\mathcal{A}$ checks whether $a_i' = a_i$ holds or not

Step D4: $\mathcal{A}$ repeats the step D1 to D3 until $a_i' = a_i$ holds

That is, $\mathcal{A}$ can guess correct ID_i and PW_i. However, $\mathcal{A}$ is still not sure they are the same identity and password. Then, $\mathcal{A}$ has to execute online guessing attack to test the correctness both. However, we use Hoeny_list to prevent online

User U_i		User U_j
Input $ID_i^{'}$ and $PW_i^{'}$,		
$a_i^{'} = h(h(ID_i) \oplus h(PW_i^{'}\|\|a_{i0}) \bmod \kappa)$,		
$a_i^{'} \stackrel{?}{=} a_i$		$t_j - t_i < \Delta t$,
$c_i \in Z_q^*, C_i = c_i P, PID_i = ID_i \oplus h(c_i X_j \|\| t_i)$,		$ID_i^* = PID_i \oplus h(x_j X_i \|\| t_i)$
$f_i = h(ID_i \|\| ID_j \|\| PID_i \|\| C_i \|\| t_i)$		$f_i^{'} = h(ID_i^* \|\| ID_j \|\| PID_i \|\| C_i \|\| t_i)$
$\sigma_i = c_i + x_i f_i \bmod q$	$\overrightarrow{M_1}$	$C_i \stackrel{?}{=} \sigma_i P - f_i^{'} X_i$
$M_1 = \{C_i, PID_i, t_i, \sigma_i\}$		$c_j \in Z_q^*, \ C_j = c_j P$
		$sk_{ji} = h(ID_i \|\| ID_j \|\| t_i \|\| t_j \| C_i c_j)$
		$f_j = h(ID_i \|\| C_i \|\| C_j \|\| sk_{ij} \|\| t_i \|\| t_j \|\| ID_j)$
		$\sigma_j = c_j + x_j f_j \bmod q$
		$M_2 = \{C_j, f_j, \sigma_j, t_j\}$
$t_i^{'} - t_j < \Delta t$	$\overleftarrow{M_2}$	
$C_j \stackrel{?}{=} \sigma_j P - f_j X_j$		
$sk_{ij} = h(ID_i \|\| ID_j \|\| t_i \|\| t_j \| c_i C_j)$		
$f_j \stackrel{?}{=} h(ID_i \|\| C_i \|\| C_j \|\| sk_{ij} \|\| t_i \|\| t_j \|\| ID_j)$		
Identical session key $sk_{ji} = sk_{ij} = h(ID_i \|\| ID_j \|\| t_i \|\| t_j \| c_i c_j P)$		

Figure 3: Login and key agreement phase.

guessing attack. As a result, the proposed pKAS can be secure against offline password guessing attack. □

Proposition 2. *The proposed pKAS scheme can be secure against online password guessing attack.*

Proof. In order to eliminate the threat of online password guessing attack, Hoeny_list is adopted in the proposed scheme. As analysis of Proposition 1, the proposed pASK can use Hoeny_list to prevent online guessing attack. Therefore, the proposed pKAS scheme can be secure against online password guessing attack. □

Proposition 3. *The proposed pKAS scheme can provide anonymous interactions among the users U_i and edge cloud sever U_j, and no adversary $\mathscr{A}$ can obtain both identity information during login and key agreement phase.*

Proof. In the login and key agreement phase of pKAS, user U_i's real identity ID_i is hidden in message $\mathrm{PID}_i = \mathrm{ID}_i \oplus h(c_i X_j \| t_i)$. If an adversary $\mathscr{A}$ can reveal the ID_i from the messages, he/she should solve the ECDLP problem because PID_i include ECDLP in their construction. Therefore, the proposed pKAS can provide anonymous interactions during user login and key agreement. □

Proposition 4. *The proposed pKAS scheme can provide forward secrecy during the session key agreement.*

Proof. Assume an adversary $\mathscr{A}$ has obtained the smart card and user's password and identity. However, $\mathscr{A}$ cannot retrieve the previously existing session key without knowing c_i because $\mathscr{A}$ should solve the ECDLP problem. Hence, the proposed pKAS scheme can give strong forward secrecy. □

Proposition 5. *The proposed pKAS scheme can be secure against forgery attack.*

Proof. In the proposed scheme, U_j can check that message M_1 has been forgery by computing $\mathrm{ID}^* = \mathrm{PID}^* \oplus h(x_j C_i \| t_i)$, $f_i' = h(\mathrm{ID}^* \| \mathrm{ID}_j \| \mathrm{PID}_i \| C_i \| t_i)$, and checking $C_i = \sigma_i P - f_i' X_i$ holds or not. U_i authenticates U_j by computing $C_j' = \sigma_j P - f_j X_j$, $\mathrm{sk}_{ji} = h(\mathrm{ID}_i \| \mathrm{ID}_j \| t_i \| t_j \| c_i C_j)$ and checking $f_j = h(\mathrm{ID}_i \| C_i \| C_j \| \mathrm{sk}_{ji} \| t_i \| t_j \| \mathrm{ID}_j)$ holds or not. When $\mathscr{A}$ modifies the message during the conversation, the tampered message cannot be verified. As a consequence, the proposed pKAS scheme can be secure against forgery attack. □

Proposition 6. *The proposed pKAS scheme can provide mutual authentication.*

Proof. In the presented scheme, U_j and U_i verify message M_1 and M_2 by checking equation $C_i = \sigma_i P - f_i' X_i$, $f_j = h(\mathrm{ID}_i \| C_i \| C_j \| \mathrm{sk}_{ji} \| t_i \| t_j \| \mathrm{ID}_j)$ hold or not, respectively. If it holds, the scheme achieves mutual authentication based on Proposition 5 that no adversary can successfully implement a forgery attack. Therefore, the presented pKAS scheme can give mutual authentication. □

Proposition 7. *The proposed pKAS can be secure against replay attack.*

Proof. In the proposed pKAS scheme, we use timestamps and random numbers to prevent replay attack. Messages M_1 and M_2 include timestamps t_i and t_j, respectively, which is a classic way to stop replay attacks. Random numbers are also used to prevent relay attack because users and server can check the validity of random number by verification algorithm each time and adversary $\mathcal{A}$ still cannot construct valid session key. Hence, the presented pKAS can be secure against replay attack. □

Proposition 8. *The proposed pKAS can be secure against impersonation attack.*

Proof. Let $\mathcal{A}$ can get U_i's smart card and know the data in the card by some way. However, $\mathcal{A}$ has to possess PW_i and ID_i into smart card to generate a legal message $M_1 = \{C_i, \mathrm{PID}_i, \sigma_i, t_i\}$. Without the two factors (PW_i and ID_i), $\mathcal{A}$ cannot compute a correct a_i to pass the verification of smart card that $\mathcal{A}$ cannot proceed to the next step to impersonate U_i to communicate with other. Therefore, the proposed pKAS can security resist impersonation attack. □

Proposition 9. *The proposed pKAS can be secure against parallel attack.*

Proof. Parallel attack usually occurs when an adversary $\mathcal{A}$ constructs a new conversation to impersonate a legal user by reusing historical messages that he/she intercepted in a public channel. However, $\mathcal{A}$ should know the parameters of messages or he/she cannot send a correct access request and gain a session key. However, $\mathcal{A}$ cannot obtain the random number that is chosen by users. As a result, the proposed pKAS can be secure against parallel attack. □

Proposition 10. *The proposed pKAS can be secure against insider attack.*

Proof. As shown in the user registration phase, user U_i send $\{\mathrm{ID}_i, X_i\}$ to U_j, where $X_i = x_i P$. Without knowing x_i, the server cannot impersonate U_i. Therefore, the proposed pKAS can be secure against insider attack. □

Proposition 11. *The proposed pKAS scheme can achieve user untraceability.*

Proof. In the proposed scheme, user U_i's real identity ID_i real identity ID_j are hidden in message $\mathrm{PID}_i = \mathrm{ID}_i \oplus h(c_i X_j \| t_i)$. Only when an adversary $\mathcal{A}$ can solve the ECDLP problem, $\mathcal{A}$ can reveal ID_i from the messages that are included by ECDLP in their construction. As a consequence, the proposed pKAS can achieve user untraceability. □

Proposition 12. *The proposed pKAS scheme can achieve key agreement.*

Proof. U_j computes his/her session key as $\mathrm{sk}_{ji} = h(\mathrm{ID}_i \| \mathrm{ID}_j \| t_i \| t_j \| C_i c_j)$, in the step A3. U_i computes his/her session key as $\mathrm{sk}_{ij} = h(\mathrm{ID}_i \| \mathrm{ID}_j \| t_i \| t_j \| c_i C_j)$, in step A4. Because $c_j C_i = c_i C_j = c_i c_j P$, U_i and U_j can compute an identical session key $\mathrm{sk}_{ji} = \mathrm{sk}_{ij}$. Therefore, the proposed pKAS scheme can achieve key agreement. □

Proposition 13. *The proposed pKAS scheme can achieve offline password change.*

Proof. As shown in introduction of the proposed scheme, offline password change phase is provided. Each user can achieve password change locally. If user inputs correct ID and PW, the correctness of ID_i and PW_i is $\kappa - 1/\kappa \approx 99.61/100$, $\kappa = 2^8$, i.e., user has a high probability of completing password local change. As a consequence, the proposed pKAS scheme can achieve offline password change. □

6.2. Performance Analysis. In this section, we compare our scheme with similar schemes in terms of security performance, communication consumption, and computing consumption. The results indicate that pKAS is more secure and effective than other similar schemes. In addition, the presented pKAS has lower communication and computation costs.

6.2.1. Comparison of Security Features. We define $F1$, $F2$, $F3$, $F4$, $F5$, $F6$, $F7$, $F8$, $F9$, $F10$, $F11$, and $F12$ are the functionality of "be secure against off-line password guessing attack," "be secure against online password guessing attack," "provide anonymous interactions," "provide forward secrecy," "be secure against forgery attack," "provide mutual authentication," "be secure against replay attack," "be secure against impersonation attack," "be secure against parallel attack," "be secure against insider attack," "achieve user untraceability," "achieve key agreement," and "achieve offline password change," respectively. In Table 2, we compare the security features of pKAS with related scheme, such as Irshad et al. [33], Tsai and Lo [35], and Kaur et al. [36].

6.2.2. Comparison of the Computation Cost. It is more convenient to define T_{BP}, T_{ME}, T_{PM}, T_{PA}, and T_{HO} are the running time (in ms) of a single bilinear pairing operation, modular exponentiation operation, elliptic curve point multiplication, point addition, and hash operation, respectively. In Table 3, we list the computing time of the server and the mobile terminal separately. The cost in Table 3 is based on [36]. We use simulation Alibaba's cloud server, and its configuration is Intel(R) Xeon(R) CPU E5-26300@ 2.30 GHz, 1 GB RAM and Ubuntu 14.04. In addition, the smartphone we use is configured with 2 GHz ARM CPU armeabi-v7a, 300 MiB RAM and Android 4.4 to simulate the mobile terminal.

Table 2: Security features comparison.

Schemes	$F1$	$F2$	$F3$	$F4$	$F5$	$F6$	$F7$	$F8$	$F9$	$F10$	$F11$	$F12$
Irshad et al. [33]	∨	×	∨	∨	×	∨	∨	×	×	×	∨	∨
Tsai and Lo [35]	×	×	∨	×	×	∨	∨	∨	∨	×	∨	∨
Kaur et al. [36]	×	×	∨	∨	×	∨	∨	∨	∨	×	∨	∨
pKAS	∨	∨	∨	∨	∨	∨	∨	∨	∨	∨	∨	∨

Note: ∨ means available; × means not available.

Table 3: Comparison of the computation cost on different devices.

Device	T_{BP}	T_{PM}	T_{PA}	T_{HO}	T_{ME}
Server	5.275	1.97	0.012	0.009	0.339
Client	48.99	19.919	0.118	0.089	3.328

Table 4: Comparison of the computation cost.

Schemes	User	Server
Irshad et al. [33]	$T_{PB} + 5T_{PM} + 2T_{PA} + 2T_{ME} + 6T_{HO} = 155.68$	$2T_{BP} + 4T_{PM} + 3T_{PA} + 2T_{ME} + 3T_{HP} = 19.171$
Tsai and Lo [35]	$5T_{PB} + 2T_{PA} + T_{ME} + 5T_{HO} = 247.309$	$2T_{BP} + 2T_{PM} + 2T_{PA} + 2T_{ME} + 5T_{HO} = 15.228$
Kaur et al. [36]	$4T_{PM} + 4T_{HO} = 80.032$	$3T_{PM} + 4T_{HO} = 5.946$
pKAS	$5P_{PM} + T_{PA} + 4T_{HO} = 100.069$	$5T_{PM} + T_{PA} + 4T_{HO} = 9.898$

Table 5: Comparison of the communication cost.

Schemes	Number of messages	Communication cost (bits)
Irshad et al. [33]	3	3072
Tsai and Lo [35]	3	3072
Kaur et al. [36]	3	1920
pKAS	2	1472

According to the time computation by each operation in Table 3, we compared the time in [33, 35, 36], and pKAS schemes, as shown in Table 4.

6.2.3. Comparison of the Communication Cost. The comparison results in Table 4 are based on assumptions such as result of hash function to be 160 bits, random number to be 128 bits, identifier to be 64 bits, time stamp to be 32 bits, and encryption/decryption and ECC point to be 320 bits. Table 5 shows a comparison of the communication cost between pKAS and other schemes [33, 35]

In summary, the presented pKAS which consumes lower communication and calculations than [33, 35]. Though the cost of [36] is lower than pKAS, the scheme cannot be secure against forgery attacks and insider attack, and its bandwidth consumption is relatively large. Furthermore, pKAS is more secure than [33, 35, 36]. So, pKAS is more suitable for user and server to verify each other.

7. Conclusion and Future Work

Aiming at the practical problems encountered in the key agreement between the user and server in the edge cloud computing environment, we propose a new password-based key agreement scheme. We use ECDLP to construct user anonymity and forward secrecy. By comparing security, communication, and calculation costs, the proposed pKAS has better security and lower cost. Furthermore, pKSA also meets all 12 security requirements.

Although pAKS is more secure and efficient than similar schemes, the lightweight key agreement scheme, such as no point multiply operation, is more favored. It is very challenging to design a secure and lightweight scheme. This will be the direction of our next research.

Data Availability

The data supporting the results of this study can be obtained from the corresponding author.

Conflicts of Interest

P. Liu is currentlty a lecturer at the Department of Computer Technology and Application, Qinghai University, Xining. Her research interest includes network protocol and protocol security (e-mail: 247750940@qq.com). Syed Hamad Shirazi is currentlty an Assistant Professor at the Department of Information Technology, Hazara University, Baffa, Pakistan. His research interest includes image processing and image security (syedhamad@hu.edu.pk). W. Liu is currently an assistant at the Department of Computer Technology and Application, Qinghai University, Xining. Her research interest includes network protocol and protocol security (e-mail: 1007759705@qq.com). Y. Xie is currently a Professor at the Department of Computer Technology and Application, Qinghai University, Xining. His research interest includes network protocol and protocol security (e-mail: mark.y.xie@qq.com).

Acknowledgments

This study was supported in part by the Science and Technology Foundation of Qinghai under grant no. 2019-ZJ-7065, the National Natural Science Foundation of China under grant no. 61572370, and Course Construction of Qinghai University under grant no. SZ19014.

References

[1] K. Kaur, S. Garg, G. S. Aujla, N. Kumar, J. J. P. C. Rodrigues, and M. Guizani, "Edge computing in the industrial internet of things environment: software-defined-networks-based edge-cloud interplay," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 44–51, 2018.

[2] X. Liang, X. Wan, X. Du, X. Chen, G. Mohsen, and C. Dai, "Security in mobile edge caching with reinforcement learning," *IEEE Wireless Communications*, vol. 25, no. 3, pp. 116–122, 2018.

[3] X. Xu, Z. Fang, L. Qi, X. Zhang, Q. He, and X. Zhou, "TripRes," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 17, no. 2, pp. 1–21, 2021.

[4] X. Xu, Q. Wu, L. Qi, W. Dou, S. B. Tsai, and M. Z. A. Bhuiyan, "Trust-aware service offloading for video surveillance in edge computing enabled internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 3, pp. 1787–1796, 2020.

[5] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) ≪ cost (signature) + cost (encryption)," in *Proceedings of the Annual International Cryptology Conference*, pp. 165–179, Springer, Santa Barbara, California, USA, August 1997.

[6] E. J. Yoon, S. B. Choi, and K. Y. Yoo, "A secure and efficiency id-based authenticated key agreement scheme based on elliptic curve cryptosystem for mobile devices," *International journal of innovative computing, information & control: IJICIC*, vol. 8, no. 4, pp. 2637–2653, 2012.

[7] D. Mishra, A. K. Das, and S. Mukhopadhyay, "A secure and efficient ecc-based user anonymity-preserving session initiation authentication protocol using smart card," *Peer-to-Peer Networking and Applications*, vol. 9, no. 1, pp. 171–192, 2016.

[8] M. F. Sabzinejad and M. A. Ahmadian, "An id-based key agreement protocol based on ecc among users of separate networks," in *Proceedings of the ISCISC International ISC Conference on Information Security and Cryptology*, Tabriz, Iran, September 2012.

[9] S. H. Islam and G. P. Biswas, "A more efficient and secure id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," *Journal of Systems and Software*, vol. 84, no. 11, pp. 1892–1898, 2011.

[10] X. Jia, D. He, N. Kumar, and K. Choo, "A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing," *IEEE Systems Journal*, vol. 14, no. 1, pp. 1–12, 2019.

[11] M. Abdalla, P. A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proceedings of the International Workshop on Public Key Cryptography*, pp. 65–84, Springer, Les Diablerets, Switzerland, January 2005.

[12] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 139–155, Springer, Kyoto, Japan, December 2000.

[13] E. J. Yoon and K. Y. Yoo, "Robust id-based remote mutual authentication with key agreement scheme for mobile devices on ecc," in *Proceedings of the 2009 International Conference on Computational Science and Engineering*, vol. 2, pp. 633–640, IEEE, Vancouver, BC, Canada, August 2009.

[14] L. Harn, W.-J. Hsin, and M. Mehta, "Authenticated diffie-hellman key agreement protocol using a single cryptographic assumption," *IEE Proceedings - Communications*, vol. 152, no. 4, pp. 404–410, 2005.

[15] Y.-M. Tseng, "Efficient authenticated key agreement protocols resistant to a denial-of-service attack," *International Journal of Network Management*, vol. 15, no. 3, pp. 193–202, 2005.

[16] E. J. Yoon and K. Y. Yoo, "New efficient simple authenticated key agreement protocol," in *Proceedings of the Computing and Combinatorics, 11th Annual International Conference, COCOON*, Kunming, China, August 2005.

[17] M. Geng and F. Zhang, "Provably Secure Certificateless Two-Party Authenticated Key Agreement Protocol Without Pairing," in *Proceedings of the International Conference on Computational Intelligence & Security*, León, Spain, November 2010.

[18] M. Hou and Q. Xu, "A two-party certificateless authenticated key agreement protocol without pairing," in *Proceedings of the The 2nd IEEE International Conference on Computer Science and Information Technology*, pp. 412–416, Beijing, China, August 2009.

[19] J. H. Yang and C. C. Chang, "An id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," *Computers & Security*, vol. 28, no. 3-4, pp. 138–143, 2009.

[20] H. Hou and S. Liu, "Cpk-based authentication and key agreement protocols with anonymity for wireless network," in *Proceedings of the International Conference on Multimedia Information Networking & Security*, Jeju Island, Korea, December 2009.

[21] A. Weimerskirch, S. Douglas, and S. C. Shantz, "Generic gf(2m) arithmetic in software and its application to ecc," in *Proceedings of the Information Security and Privacy, 8th Australasian Conference, ACISP 2003*, Wollongong, Australia, July 2003.

[22] S. U. Nimbhorkar and L. G. Malik, "Exploration of schemes for authenticated key agreement protocol based on elliptic curve cryptosystem," in *Proceedings of the 2013 6th International Conference on Emerging Trends in Engineering and Technology (ICETET)*, Nagpur, India, December 2013.

[23] S. M. Bellovin and M. Merritt, "Encrypted key exchange: password-based protocols secure against dictionary attacks," in *Proceedings of the IEEE Symposium on Security & Privacy*, Oakland, CA, USA, May 1992.

[24] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, 1981.

[25] J. Xu, W. T. Zhu, and D. G. Feng, "An improved smart card based password authentication scheme with provable security," *Computer Standards & Interfaces*, vol. 31, no. 4, pp. 723–728, 2009.

[26] S. K. Sood, A. K. Sarje, and K. Singh, "An improvement of xu et al.'s authentication scheme using smart cards," in *Proceedings of the ACM bangalore annual conferenceCOMPUTE 2010*, Banglore, India, January 2011.

[27] B. L. Chen, W. C. Kuo, and L. C. Wuu, "Robust smart-card-based remote user password authentication scheme,"

International Journal of Communication Systems, vol. 27, no. 2, 2014.

[28] X. Li, J. Niu, M. K. Khurram, and J. Liao, "An enhanced smart card based remote user password authentication scheme," *Journal of Network and Computer Applications*, vol. 36, no. 5, pp. 1365–1371, 2013.

[29] W. B. Hsieh and J. S. Leu, "Exploiting hash functions to intensify the remote user authentication scheme," *Computers & Security*, vol. 31, no. 6, pp. 791–798, 2012.

[30] H. B. Tang, X. S. Liu, and L. Jiang, "A robust and efficient timestamp-based remote user authentication scheme with smart card lost attack resistance," *International Journal on Network Security*, vol. 15, no. 6, pp. 446–454, 2013.

[31] A. K. Awasthi, K. Srivastava, and R. C. Mittal, "An improved timestamp-based remote user authentication scheme," *Computers & Electrical Engineering*, vol. 37, no. 6, pp. 869–874, 2011.

[32] E. J. Yoon, K. Y. Yoo, and K. S. Ha, "A user friendly authentication scheme with anonymity for wireless communications," *Computers & Electrical Engineering*, vol. 37, no. 3, pp. 356–364, 2011.

[33] A. Irshad, M. Sher, H. F. Ahmad, B. A. Alzahrani, and R. Kumar, "An improved multi-server authentication scheme for distributed mobile cloud computing services," *Ksii Transactions on Internet & Information Systems*, vol. 10, no. 12, pp. 5529–5552, 2016.

[34] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," *Future Generation Computer Systems*, vol. 81, pp. 557–565, 2018.

[35] J. L. Tsai and N. W. Lo, "A privacy-aware authentication scheme for distributed mobile cloud computing services," *IEEE Systems Journal*, vol. 9, no. 3, pp. 805–815, 2017.

[36] K. Kaur, S. Garg, G. Kaddoum, M. Guizani, and D. Jayakody, "A lightweight and privacy-preserving authentication protocol for mobile edge computing," in *Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM)*, IEEE, Waikoloa, HI, USA, December 2020.

[37] L. Xiong, D. Peng, T. Peng, and H. Liang, "An enhanced privacy-aware authentication scheme for distributed mobile cloud computing services," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 12, pp. 6169–6187, 2017.